

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平8-63532

(43)公開日 平成8年(1996)3月8日

(51)Int.Cl.⁶

識別記号

庁内整理番号

F I

技術表示箇所

G 0 6 F 19/00

G 0 7 F 19/00

G 0 6 F 15/ 30

M

C

G 0 6 F 15/ 30

L

審査請求 未請求 請求項の数38 F D (全 13 頁) 最終頁に続く

(21)出願番号 特願平7-187802

(22)出願日 平成7年(1995)6月30日

(31)優先権主張番号 0 8 / 2 6 9 2 0 5

(32)優先日 1994年6月30日

(33)優先権主張国 米国 (U S)

(71)出願人 590005645

タンデム・コンピュータズ・インコーポ
レイテッド

アメリカ合衆国カリフォルニア州95014-
0709クパチーノ, ノース・タンタウ・アヴ
ェニュー・10435

(72)発明者 ダブリュ・デイル・ホプキンス

アメリカ合衆国 カリフォルニア 95020,
ギルロイ, リック・ドライブ 2425

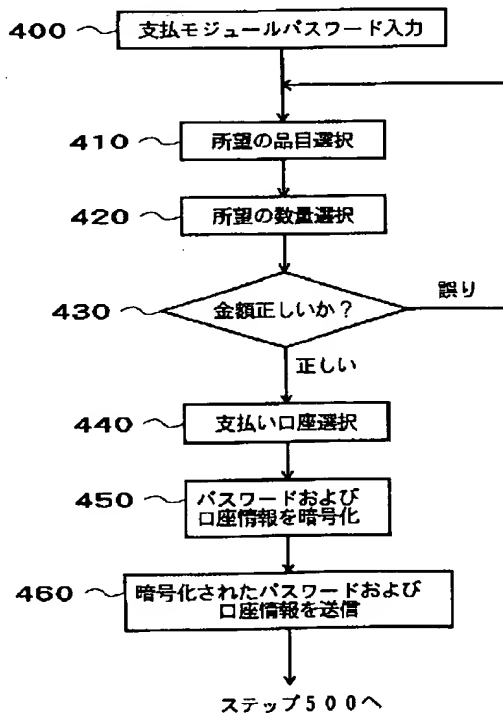
(74)代理人 弁理士 飯塚 義仁

(54)【発明の名称】 遠隔金融取引システム

(57)【要約】

【目的】 高度に安全化された遠隔金融取引を可能にする。

【構成】 遠隔金融取引を行うシステムは、メモリにアクセス可能で、例えば、対話型のネットワークを介してオフサイト処理システムと通信可能な支払いモジュールを使用する。この支払いモジュールは、メモリに格納された支払い口座情報、および、これに対応する個人識別情報にアクセスする。ユーザは、所望の遠隔金融取引、および、アクセスすべき支払い口座を選択することができる。前記個人識別情報および必要な支払い口座情報は、前記メモリから読み出されて暗号化され、そして、最終的に、前記対話型のネットワークを介して、前記口座を維持する金融機関に送られる。前記金融機関は、選択された遠隔金融取引にを受け入れるか、または、拒絶するかを決定を行い、前記対話型のネットワークを介して、受入れまたは拒絶を示すメッセージをユーザに送ることができる。



1

【特許請求の範囲】

【請求項 1】 少なくとも 1 つの支払い口座および少なくとも 1 つのパスワードを示すデータを格納するメモリにアクセスし且つオフサイト処理システムと通信する支払いモジュールを使用して、遠隔金融取引を行う方法であって、

前記支払いモジュールを使用して、前記オフサイト処理システムに対して、前記メモリに格納されたデータに基づき、支払い口座を特定する情報を提供することと、前記支払いモジュールを使用して、前記オフサイト処理システムに対して暗号化されたパスワードを提供することとを具備する方法。

【請求項 2】 前記支払い口座を特定する情報を提供することに先行して、前記支払いモジュールを初期化するステップを更に具備し、該初期化するステップが各所望の支払い口座ごとに 1 回だけ実行されるべきものであり、かつ、該初期化するステップが、

少なくとも 1 つの支払い口座を特定する情報を前記メモリに格納するステップと、

前記支払いモジュールに格納された情報によって特定される各支払い口座が、これに対応して格納された少なくとも 1 つの暗号化されたパスワードを有するように、該少なくとも 1 つの暗号化されたパスワードを前記メモリに格納するステップとを含むことを特徴とする請求項 1 に記載の方法。

【請求項 3】 アクセスパスワードを前記メモリに格納するステップをさらに含む請求項 2 に記載の方法。

【請求項 4】 前記暗号化されたパスワードを提供することに先行して、該パスワードを暗号化するためのステップを更に具備することを特徴とする請求項 2 に記載の方法。

【請求項 5】 前記暗号化するステップが、各取引ごとに独特のキーを使用して行われることを特徴とする請求項 4 に記載の方法。

【請求項 6】 前記支払い口座を特定する情報を提供することに先行して、前記支払い口座を特定する情報を暗号化するステップを更に具備することを特徴とする請求項 1 に記載の方法。

【請求項 7】 前記支払い口座を特定する情報を暗号化するステップが、各取引ごとに独特のキーを使用して行われることを特徴とする請求項 6 に記載の方法。

【請求項 8】 前記支払い口座を特定する情報を提供することの前に、

前記支払いモジュールに対してアクセスパスワードを入力するステップと、

正しいアクセスパスワードが入力されたか否かを判定するステップとを更に具備し、遠隔金融取引を実行する前に、正しいアクセスパスワードが入力されなければならないようにしたことを特徴とする請求項 1 に記載の方法。

2

【請求項 9】 支払い口座を選択するステップを更に具備し、

前記支払い口座を特定する情報を提供することは、当該支払い口座を選択するステップで選択された支払い口座を特定する情報を提供することであり、

前記暗号化されたパスワードを提供することは、当該支払い口座を選択するステップで選択された支払い口座に対応する暗号化されたパスワードを提供することである請求項 1 に記載の方法。

10 【請求項 10】 前記支払い口座を特定する情報を提供することの前に、ユーザに対して金融取引の選択肢を提供するステップを更に具備することを特徴とする請求項 1 に記載の方法。

【請求項 11】 前記ユーザに対して金融取引の選択肢を提供するステップの後に、1 つの金融取引を選択するステップを更に具備することを特徴とする請求項 10 に記載の方法。

20 【請求項 12】 前記オフサイト処理システムから前記支払いモジュールに対して、選択された金融取引に関する受入れメッセージまたは拒絶メッセージを送るステップを更に具備することを特徴とする請求項 1 に記載の方法。

【請求項 13】 前記支払い口座を特定する情報を提供することが、ケーブルテレビ送信システムに対して支払い口座を特定する情報を提供するステップを含む請求項 1 に記載の方法。

30 【請求項 14】 前記支払い口座を特定する情報を提供することが、ATMネットワークに対して支払い口座を特定する情報を提供するステップを含む請求項 1 に記載の方法。

【請求項 15】 前記支払い口座を選択するステップが、表示画面に、支払い口座をリストした図式表示を提供することと、

前記表示にリストされた支払い口座の中から 1 つの支払い口座を選ぶこととを含む請求項 9 に記載の方法。

【請求項 16】 前記 1 つの支払い口座を選ぶことが、入力装置を使用して、前記表示画面に表示されたインジケータ記号を、所望の支払い口座に対応する位置に動かすことにより行われる請求項 15 に記載の方法。

40 【請求項 17】 表示装置においてメニューおよびプロンプトを表示することと、前記表示されたメニューおよびプロンプトを使用して遠隔金融取引を実行することとを更に具備する請求項 1 に記載の方法。

【請求項 18】 前記オフサイト処理システムによって、前記遠隔金融取引を受入れるかまたは拒絶するかについての決定を行うステップを更に具備する請求項 1 に記載の方法。

50 【請求項 19】 前記支払い口座を特定する情報を提供

3

することに先行して、支払い口座を選択するステップを更に具備する請求項1に記載の方法。

【請求項20】 前記暗号化されたパスワードが、前記メモリに格納された少なくとも1つのパスワードを示すデータに基づくものである請求項1に記載の方法。

【請求項21】 前記少なくとも1つの支払い口座を示すデータが、口座維持機関からの少なくとも1つの支払い口座に対応するデータであり、前記支払い口座を使用させることを前記口座維持機関により許可するステップを更に具備することを特徴とする請求項1に記載の方法。

【請求項22】 データを格納するためのメモリにアクセス可能な支払いモジュールを備えた遠隔金融取引を行うための装置を初期化する方法であって、前記メモリに少なくとも1つの支払い口座を特定する情報を格納するステップと、前記支払いモジュールに格納された情報によって特定される各支払い口座が、これに対応する少なくとも1つの暗号化されたパスワードを有すように、該少なくとも1つの暗号化されたパスワードを生成すべく該少なくとも1つのパスワードを暗号化するステップと、前記メモリに前記少なくとも1つの暗号化されたパスワードを格納するステップとを具備する方法。

【請求項23】 前記暗号化するステップが、少なくとも1つのペーパー暗号手段を使用して行われる請求項22に記載の方法。

【請求項24】 前記少なくとも1つの支払い口座を特定する情報が、口座維持機関からの少なくとも1つの支払い口座に対応するデータであり、前記支払い口座を前記支払いモジュールを使用して行う金融取引に使用させることを前記口座維持機関により許可するステップを更に具備する請求項22に記載の方法。

【請求項25】 オフサイト処理システムと通信する遠隔金融取引を行うための装置であって、前記オフサイト処理システムと通信することによって、遠隔金融取引を行う支払いモジュールと、少なくとも1つの支払い口座と少なくとも1つのパスワードとを示すデータを格納するために、前記支払いモジュールによってアクセス可能なメモリとを具備する遠隔金融取引を行うための装置。

【請求項26】 データを伝送するための対話型のネットワークを更に具備しており、前記支払いモジュールが、データを送受するために前記対話型のネットワークと通信し、前記オフサイト処理システムが、前記対話型のネットワークを使用して、前記支払いモジュールに対してデータを送受する請求項25に記載の装置。

【請求項27】 前記メモリが、前記支払いモジュールの一構成要素である請求項25に記載の装置。

【請求項28】 前記支払いモジュールが、

4

前記オフサイト処理システムに対して、前記メモリに格納されたデータに基づき、支払い口座を特定する情報を提供する手段と、

前記オフサイト処理システムに対して、暗号化されたパスワードを提供する手段とを有するものである請求項26に記載の装置。

【請求項29】 前記パスワードを暗号化するための手段を更に具備する請求項26に記載の装置。

【請求項30】 前記暗号化するための手段が、各取引ごとに独特のキーを使用して暗号化を行う請求項29に記載の装置。

【請求項31】 前記支払いモジュールに対してアクセスパスワードを入力する手段と、正しいアクセスパスワードが入力されたか否かを判定する手段とを更に具備し、遠隔金融取引を実行する前に、正しいアクセスパスワードが入力されなければならないようにしたことを特徴とする請求項25に記載の装置。

【請求項32】 支払い口座を選択する手段を更に具備し、

前記支払い口座を特定する情報を提供する手段が、前記選択する手段によって選択された支払い口座を特定する情報を提供するものであり、

前記暗号化されたパスワードを提供する手段が、前記選択する手段によって選択された支払い口座に対応する暗号化されたパスワードを提供するものである請求項28に記載の装置。

【請求項33】 ユーザに対して金融取引の選択肢を提供する手段を更に具備する請求項28に記載の装置。

【請求項34】 前記対話型のネットワークがケーブルテレビ送信システムである請求項26に記載の装置。

【請求項35】 前記対話型のネットワークがATMネットワークである請求項26に記載の装置。

【請求項36】 前記対話型のネットワークがEFT-POSネットワークである請求項26に記載の装置。

【請求項37】 前記支払いモジュールによって与えられる指示に応じて動作する表示画面を更に具備する請求項25に記載の装置。

【請求項38】 入力装置と、該入力装置を使用して、前記表示画面に表示されたインジケータ記号を動かす手段とを更に具備する請求項37に記載の装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】この発明は、遠隔位置とオフサイト(off-site: 現場から離れた)取引記録位置または取引処理位置との間で通信を行う場合において、前記遠隔位置から所望の金融取引を安全化して実行するための方法および装置、すなわち遠隔金融取引システム、に関する。

【0002】

【従来の技術】遠隔操作によって行われる金融取引の安全性および秘密を維持するための技術は、様々なものが提案されている。このような技術は、一般に、個人識別番号またはPIN (Personal Identification Number) と呼ばれる秘密のパスワードを使用するものである。一般に、取引を行う場合、前記個人識別番号は、読取り装置によって物理的に走査される第2の形態の識別コードと共に使用される。

【0003】遠隔取引のための周知技術の一例としては、銀行のATM (自動預金支払機) や、販売時点での電子的資金移動端末 (“EFT-POS” 端末) がある。典型的なATMおよびEFT-POS端末は、ユーザが磁気コードを有するカードを挿入することを必要とする。例えば、ユーザの名前、口座番号、カード有効性確認値 (“CVV”) および有効期限終了日を含むトラック1の情報が読み取られる。さらに、典型的には、取引を行うためには、ユーザが前記個人識別番号を入力することが要求される。また、典型的には、前記個人識別番号は、銀行またはクレジットカード会社などの登録機関によって割り当てられる。1つの方法として、前記登録機関が、個人識別番号をユーザに割り当てる。また、他の方法として、ユーザが、自分で個人識別番号を選択することができる。自分で個人識別番号を選択する場合、ユーザは、自ら登録機関を訪問して選択することができる。また、典型的には、前記ATMは、ユーザの家から離れた所に在る。

【0004】ATMネットワークおよびEFT-POSネットワークも知られている。このようなネットワークの1つは、ANSI X9.24規格に記載されている。このようなネットワークにおいて、複数の異なる金融機関のATM (またはEFT-POS) は、中央の処理機関を介して接続されている。このようなネットワークを使用して、例えば、特定の銀行に口座を有するユーザは、異なる銀行から、預金引出しなどの金融取引を行うことができる。このようなネットワークは、広く知られており、“NYCE”、“PLUS”、“CIRRUS”などの商品名を有する。典型的なネットワークにおいて、1つの銀行のATMは、該銀行のデータ処理装置に接続されている。そのネットワークに接続された他の銀行も、同様なATM構成を有する。前記ネットワークに接続された各銀行のデータ処理装置は、中央の処理機関に接続されている。このようにして、前記中央の処理機関は、前記ネットワークに接続された適当な銀行に対して取引要求を送るルータ (router) または金融ネットワークスイッチとして動作する。

【0005】しかし、上記ATMは、これまで、様々な形態の悪意の攻撃を受けてきた。例えば、ユーザは、自分で、暗号化されていない形態の個人識別番号をシステムに入力するので、該個人識別番号はアクセス可能である。典型的には、ATM端末では、ATMネットワークを介し

て該端末から伝送される前に個人識別番号を暗号化するが、多数の個人識別番号について1つの暗号化キーを使用する。このため、予め知られている個人識別番号が攻撃用の基礎番号として使用される辞書攻撃 (dictionary attack) が使用されている。前記予め知られている暗号化された個人識別番号が (例えば、これに対応する非暗号化口座情報を検出することによって) 傍受され、そして、これと異なる口座に対応する同一の暗号化された個人識別番号が傍受された場合においては、両者には同一の暗号化キーが使用されているので、後者の口座の個人識別番号を知ることができる。

【0006】前記登録機関において自ら行う代りに、遠隔地において個人識別番号を選択して暗号化する技術としては、様々なものが知られている。ペーパー暗号化システムは、米国特許第4,870,683号および第4,885,779号に開示されている。このペーパー暗号化システムを使用して、ユーザは、在宅のまま個人識別番号を選択して暗号化し、該個人識別番号を前記登録機関に郵送することができる。また、ユーザは、電話線を介して、暗号化された個人識別番号を伝送することもできる。遠隔地において個人識別番号を選択して暗号化するための他の技術において、ユーザは、(例えば、モデム通信を介して) 電子的に前記暗号化システムと通信して個人識別情報を送信し、その代りに、暗号化された個人識別番号を受信する。このようなシステムは、この発明の譲受人と同一の譲受人に譲渡された現在係属中の米国特許出願第08/029,833号に記載されている。

【0007】様々な非暗号化、在宅購入システムが知られている。このようなシステムの一例はテレビホームショッピングである。典型的なテレビホームショッピングシステムには、米国のQVCネットワークおよびHome Shopping Channelがある。このようなテレビホームショッピングシステムにおいて、放送番組はテレビ受像機によって受信される。典型的には、前記放送番組の内容には、販売される製品の説明、映像表示、価格および注文方法の案内等が含まれる。典型的には、ユーザには、注文するための無料の電話番号が提供される。ユーザは、様々な情報が受注者側に与えらる必要があるクレジットカードを使用して、注文することができる。

【0008】

【発明が解決しようとする課題】しかし、電話線は傍受または盗み聞きなどによる悪意の攻撃を受けやすいので、この種のシステムでは、安全が保証されない。同様に、クレジットカード情報は暗号化されていないので、悪意の攻撃者は、電話線を介して、または、注文を受け取る施設において、クレジットカード情報を入手できる。

【0009】他の種類のテレビサービスは、テレビ受像機を介して、安全化されていない対話型のオーダ (発注) 方式を提供する。このようなサービスは、一般に、

7

ホテルにおいて提供され、ホテルの客室からの遠隔チェックアウト処理を可能にする。このようなサービスにおいて、ホテルの客には、客室内のテレビ受像機を介して、様々なチェックアウトオプション（選択肢）が提供される。例えば、客に対して、食事、電話料金等のその客室に関する料金をチェックすること、および、ホテルロビーに在るフロントデスクに自ら行くことを必要としない自動チェックアウトを含む様々なオプションが与えられる。これらのオプションは、典型的にはケーブルを介してテレビ画面に現れるメニューに表示される。客は、典型的な手持ち型の赤外線コントローラ等の遠隔制御すなわちリモコン装置を使用して、そのメニューをスクロールし、選択する。同様に、前記手持ち型のコントローラを使用して、異なるメニューオプションが選択される。

【0010】しかし、このような方式は、テレビを介して直接に支払いを行うことを可能にしない。典型的には、ホテル側は、フロントデスクでのチェックイン時に、クレジットカード（および、任意に、追加的な身元確認証）の提示によって、料金の前払いをしてもらう。さらに、この方式は、ケーブルシステムによってテレビ信号を傍受することによる、または、客のクレジットカード情報に関するホテル記録にアクセスすることによる悪意の攻撃を受け易い。

【0011】テレビによる他の対話型のオーダ方式は、視聴ごと支払い（pay-per-view）方式の有料映画を注文しまたはこれを遮断するために使用される。ホテルの客室内に提供されるようなこの種の視聴ごと支払いサービスの一例は、ユーザが（その料金はホテルの請求書に付加されるが）様々な映画の中からリクエストすべきものを選択すること、および、ある特定の映画またはすべての映画を遮断することを可能にする。チェックアウト方式と同様に、ユーザは、典型的な手持ち型のテレビまたはビデオカートリッジレコーダ（VCR）のリモコン装置を使用して、メニュー画面をスクロールして選択を行う。しかし、この場合も、ユーザは直接に支払いを行うことができない。その代わりに、料金はホテルの請求書またはケーブル請求書に付加される。チェックアウト方式と同様に、この映画オーダ方式は悪意による攻撃を受け易い。

【0012】コンピュータ掲示板サービスは、他の形態の在宅購入方式を提供する。このようなサービスの一例は、米国オハイオ州、Columbus、5000 Arlington Centre Blvd.のCompuserveである。この方式において、典型的には、ユーザは、パソコンから遠くのコンピュータシステムに通信する。遠くのコンピュータと前記掲示板サービスとの間での電話による交信を開始するために、典型的には、モデムが使用される。ユーザは、様々なサービスおよび販売される製品をざっと一覧するオプションを利用できる。支払いは、典型的には、クレジットカード

8

ドによって、または、小切手を郵送することによって行われる。しかし、このような方式も、電話の盗み聞きおよび傍受、前記コンピュータ掲示板サービスに対する直接的なアクセス、遠くからのハッカー攻撃、または、郵便に対するアクセス等による、悪意の攻撃を受け易い。この発明は上述の点に鑑みてなされたもので、高度に安全化された遠隔金融取引を行う方法および装置、すなわち遠隔金融取引システム、を提供しようとするものである。

10 【0013】

【課題を解決するための手段】上記目的を達成するために、この発明は、少なくとも1つの支払い口座および少なくとも1つのパスワードを示すデータを格納するメモリにアクセスし且つオフサイト処理システムと通信する支払いモジュールを使用して、遠隔金融取引を行う方法であって、前記支払いモジュールを使用して、前記オフサイト処理システムに対して、前記メモリに格納されたデータに基づき、支払い口座を特定する情報を提供することと、前記支払いモジュールを使用して、前記オフサイト処理システムに対して暗号化されたパスワードを提供することとを具備することを特徴とするものである。また、この発明は、データを格納するためのメモリにアクセス可能な支払いモジュールを備えた遠隔金融取引を行うための装置を初期化する方法であって、前記メモリに少なくとも1つの支払い口座を特定する情報を格納するステップと、前記支払いモジュールに格納された情報によって特定される各支払い口座が、これに対応する少なくとも1つの暗号化されたパスワードを有するように、該少なくとも1つの暗号化されたパスワードを生成すべく該少なくとも1つのパスワードを暗号化するステップと、前記メモリに前記少なくとも1つの暗号化されたパスワードを格納するステップとを具備することを特徴とするものである。

【0014】さらに、この発明は、オフサイト処理システムと通信する遠隔金融取引を行うための装置であって、前記オフサイト処理システムと通信することによって、遠隔金融取引を行う支払いモジュールと、少なくとも1つの支払い口座と少なくとも1つのパスワードとを示すデータを格納するために、前記支払いモジュールによってアクセス可能なメモリとを具備することを特徴とするものである。

40 【0015】

【作用】この発明は、パスワードによる安全策を使用する遠隔金融取引システムを提供し、且つ、個人のパスワードを選択して実行する安全方法を提供することによって、既知の技術および装置が持つ不利な点を大幅に解消する。この発明は、例えば初期化された遠隔制御装置つまりリモコン装置のような支払いモジュールを使用して、対話型のネットワークを介して、遠隔金融取引を行う方法および装置を提供する。より詳しくは、商品ま

50

たはサービスの購入のような金融取引を行うために、前記支払いモジュールは、ケーブルシステムに接続されたテレビ等の、対話型のネットワークに接続された受信装置と通信する。他の実施例において、前記支払いモジュールは、前記リモコン装置から分離してもよい。

【0016】好ましい実施例において、番組提供者は、無線または有線のテレビを介して、販売するための商品およびサービスを提供する。代案として、商品またはサービスは、人工衛星送信または電話線によるコンピュータ通信のような、その他の形態の対話型ネットワークを介して提供されてもよい。ユーザは、番組を見、前記制御装置を使用して、様々な商品またはサービスを任意にスクロール表示させる。ユーザが購入すなわち金融取引を行いたい場合、メニューなどの様々な選択肢が画面にグラフィック表示される。購入のような特定の金融取引が所望の場合、ユーザは、前記グラフィック表示から所望の選択肢を選ぶ。ユーザは、前記制御装置にパスワード（ここでは、個人識別番号（PIN））を入力するよう案内される。このように個人識別番号を入力すると、前記支払いモジュールが始動する。そして、ユーザは、予め初期化された該ユーザのクレジットカードまたはデビットカードなどの、所望の支払い方法を選択する。

【0017】暗号化されていない個人識別番号に対応する暗号化された個人識別番号は、前記支払いモジュールに格納される。好ましくは、前記個人識別番号を前記ネットワークに送る前に、前記支払いモジュールは、例えばANSI X9.24規格に記載されているような、取引ごと

に発生される独特のキー技術（“DUKPT”技術）を使用して、既に暗号化されている個人識別番号をさらに暗号化する。

【0018】そして、前記支払いモジュールは、前記対話型のネットワークを介して、前記暗号化された個人識別番号（すなわち、二重に暗号化された個人識別番号）を、（クレジットカードまたはデビットカードのトラック1またはトラック2のデータのような）関連データと共に送る。こうして、該ネットワークのホストシステムは、ユーザがカードを入手した銀行のような適当な金融機関に対してこの情報を送る。そして、前記所望の取引要求は、前記ネットワークを介してカード発行機関に送られ、該カード発行機関では、前記暗号化された個人識別番号を解読し、前記取引を受入れるかまたは拒絶するかについて決定する。この受入れまたは拒絶を示すメッセージは、ユーザに返され、該ユーザの表示画面に表示される。

【0019】好ましい実施例において、前記支払いモジュールは、そのDUKPTキーによって初期化される。所望のクレジットカードまたはデビットカードに対応する識別情報も、前記支払いモジュールに入力される。好ましくは、この情報は、ユーザによって前記支払いモジュール

ルに入力される数字列として入力される。典型的には、これは、各所望のカードごとに一度だけ行われる必要があり、ユーザのモニタに現れる図式的なプロンプトおよび指示によって補助される。また、好ましくは、ユーザは、各カードに対応する暗号化された個人識別番号を入力する。このように個人識別番号を暗号化するために、上述したペーパー暗号化手段を使用してよい。前記暗号化キーは、前記支払いモジュール内に維持されるものではない。

10 【0020】また、好ましくは、ユーザは、前記支払いモジュールに対するアクセスを制御するために使用される個人的なアクセスパスワードを選択するよう要求される。多くのユーザは、そのユーザ自身のカードに対するアクセスを制御する個人的なアクセスパスワードを使用することによって、同一の支払いモジュールを使用することができる。この発明を利用することによって、例えばATMネットワークのような既存のシステムに必要な磁気片リーダを使用する必要なしに、安全な取引が行われる。このように、磁気片を読み取るために必要な装置が必要でないので、前記支払いモジュールは磁気片リーダほどには嵩ばらない。

【0021】暗号化されていない個人識別番号は、前記支払いモジュールおよび対話型のネットワークの両方において決して明かされないので、このシステムは、ATMネットワークまたは小売販売時点端末で通常提供されるものより、大きな安全性を提供する。前記個人識別番号は、前記支払いモジュールにおいて暗号化された形態で格納され、暗号化されていない形態では前記ネットワーク上に伝送されない。解読キー（“キー”）は、前記支払いモジュール内に維持されない。その代りに、前記キーは、カード発行機関にのみ維持され、前記ネットワーク内のその他のいかなるエンティティにも所有されない。

【0022】さらに、この発明の前記支払いモジュールは、既存のATMネットワークおよび販売時点ネットワークと完全に互換性がある。暗号化およびパスワードによる保護を使用することによって、一層の安全が保証される。さらに、この発明の取引システムは、該遠隔金融取引システムが個々の銀行によって維持される口座を利用してよいか否かについての裁量、および、任意の使用条件を、個々の銀行（および、その他の支払い口座維持機関）に対して提供する。

【0023】さらに、この発明の装置は、遠隔取引を行うための現在の手段に比べて、よりコンパクトでコストが安い。例えば、磁気片リーダおよび（ユーザの既存の表示器以外の）表示画面のスペースおよびコストを削除できる。

【0024】

50 【実施例】以下、添付図面を参照してこの発明の実施例を詳細に説明する。図1は、この発明の一実施例に係る

在宅支払いシステムを示す図である。ユーザ 10 は、支払いモジュール 20 を操作する。図示した実施例において、前記支払いモジュール 20 は、受信機と通信するリモコン装置を含んでいる。該受信機との通信は、ワイア等を介して通信リンク 30 または無線送信によって実現される。任意の形態の無線通信リンクを使用してもよい。テレビのリモコン装置に代表される赤外線送信方式が好ましいが、他の形態の無線送信方式を使用してもよい。例えば、マイクロウェーブ、音波または電波による送信方式を使用してもよい。

【0025】前記支払いモジュールおよびリモコン装置は、図 1 に示すように同一の装置に統合されているのが好ましい。しかし、前記支払いモジュールは、他の装置部品に組込まれていてもよいし、独立型の装置であってもよい。前記支払いモジュールが他の装置部品に組込まれている場合、リモコン装置を使用して該支払いモジュールと通信するようにしてもよい。また、代案として、キーボード、ジョイスティック、マウス、または、その他の形態のコントローラを使用してもよい。この支払システムのその他の家内に置かれる構成要素としては、テレビ画面のような視覚的な表示器 40、および、対話型（インタラクティブ：interactive）通信ネットワーク 80（図 2）にアクセスするためのコネクタ 50 が含まれる。

【0026】様々な形態の表示器 40 を使用してよい。テレビが使用されるのが好ましいが、コンピュータのモニタ、LCD またはその他のディスプレイを使用してもよい。同様に、例えばオーディオインターフェイスまたは電話のような、非視覚的なディスプレイを使用してもよい。

【0027】好ましい実施例において、前記コネクタ 50 は、テレビのケーブルシステムを接続するために使用されるタイプのケーブル接続部である。前記対話型通信ネットワーク 80 がケーブルシステムである場合、該ネットワーク 80 で通信を行うため、典型的にはケーブル箱のようなネットワークインターフェイス 60 が使用される。図 1 に示すように、前記コネクタケーブル 50 は、前記ネットワークインターフェイスつまりケーブル箱 60 に接続されている。

【0028】前記対話型通信ネットワーク 80 は、ユーザ側のローカルシステム 100 から遠隔のシステム 200 にデータを送信でき、また、遠隔のシステム 200 から該ネットワーク 80 を介してユーザがデータを受信できるようにする任意のタイプのネットワークであってよい。前記テレビケーブルシステムの他に、ATM ネットワーク、広域コンピュータネットワーク、ローカルエリアコンピュータネットワーク、および、電話線を介したコンピュータ通信などの様々な形態の対話型ネットワークが知られている。この発明の一実施例において、前記対話型通信ネットワーク 80 は、ATM ネットワークによってインターフェイス接続されたケーブルテレビシステム

を含む。

【0029】図 1 の実施例において、前記支払いモジュール 20 は、リモコン装置内にあって、前記ケーブル箱 60 と通信する。該ケーブル箱 60 は、前記コネクタ 50 を介して前記ネットワーク 80 に対して所望のデータを送信する。また、前記ケーブル箱 60 は、前記ネットワーク 80 およびコネクタ 50 を介して、遠隔のシステム 200 からデータを受信する。前記ケーブル箱 60 によって受信されたデータは、前記支払いモジュール 20 もしくは表示器 40、または、これら両方に送られる。

【0030】ユーザ側のローカルシステム 100 は、前記ネットワーク 80 を介して送られる番組作成ソース 110 からの番組を受け取る。図示例において、ネットワークインターフェイスが、テレビアンテナケーブルのような通信線 70 を介して、前記番組を受け取り、これを前記表示器 40 に送る。前記番組は、消費者に様々な商品およびサービスを売るための在宅小売システムに向けられた番組のみならず、様々なテレビ局に関する情報を含んでいてよい。使用時において、ユーザ 10 は、前記ケーブルテレビに基づいた実施例の場合にはテレビチャンネルを変えることによって、また、前記コンピュータに基づいた実施例の場合にはメニューを選択することによって、前記ローカルシステム 100 によって受信された様々な番組を選択する。

【0031】図 3 に示すような他の実施例において、前記支払いモジュール 20 は、リモコン装置 22 として示されているコントローラ 22 から分離している。前記支払いモジュール 20 は、有線または無線の接続手段 32 によって表示器 40 と通信し、接続線 52、50 を介して前記ネットワークと通信する。ケーブル箱のようなインターフェイスユニット 60 は、線 50 を介して前記ネットワークと通信し、線 70 を介して前記表示器 40 と通信する。

【0032】図 4 の実施例において、前記支払いモジュールは、前記表示器と共に、1 つの支払いモジュール／表示器ユニット 42 に統合されている。該支払いモジュール／表示器ユニット 42 は、コネクタを介して直接に、または、図示のように通信線 70、インターフェイス 60 および接続線 50 を介して、前記ネットワークと通信する。

【0033】好ましい支払いモジュール 20 は、ユーザによる入力が可能で、および、（表示器 40 またはネットワークインターフェイス 60 のような）受信装置に対して出力信号を送信することが可能な手持ち型の装置である。図 5 に示すような 1 つの実施例において、支払いモジュール 20 は、キーパッド 23 のようなユーザ入力装置を含んでいる。好ましくは、前記キーパッド 23 は、テレビのリモコン装置に使用される例えば“0”～“9”の典型的な入力キー、チャンネル制御キーおよび音量制御キーを有する。これらに代えて、または、これ

らに加えて、前記支払いモジュール20は、ライトペン、マウスまたはタッチスクリーン表示器のような他の入力装置を有していてもよい。前記キーパッド23は、前記支払いモジュール20の他の構成要素と対話を行うために、データバス25と通信する。前記支払いモジュール20の機能を制御するために、マイクロプロセッサ26のようなデータプロセッサが含まれている。(プログラマブル読み出し専用メモリ)のようなプログラム/情報格納装置28は、ユーザの支払い口座、および、前記支払いモジュールの処理を制御するソフトウェアに関するデータを格納するものである。他の形態のメモリ装置が使用されてもよい。例えば、磁気格納装置(すなわち、ディスクドライブ)、光学的格納装置または任意のソリッドステート格納装置が、使用されてもよい。前記メモリ装置は、(インターフェイス装置、表示器またはオフサイト位置のメモリのように)前記支払いモジュールから遠く離れていてもよい。出力アダプタ29は、前記支払いモジュール20と前記受信装置との間における遠隔通信を可能にする。

【0034】使用時において、前記支払いモジュールは、支払い口座のパスワード(例えば、“個人識別番号(PIN)”)、および、所望の支払い口座に関するその他の情報によって、初期化されなければならない。クレジットカード口座、デビットカード口座または当座預金口座のような、任意の支払い口座を使用してよい。同様に、前記支払いモジュールを、“支払いモジュールパスワード”と呼ばれるアクセスパスワードによって初期化することが好ましい。

【0035】この初期化のための好ましい第1のステップは、前記支払いモジュールを、前記DUKPT技術と互換性を有する暗号キーによって初期化することである。好ましくは、この初期化は、遠隔金融取引サービスを提供するエンティティのようなサービス提供者によって行われる。こうして、前記サービス提供者は、暗号解読キーを維持するか、または、該解読キーを適当な機関に与える。

【0036】前記初期化のための好ましい第2のステップは、前記支払いモジュールを、該モジュール用に選択される各支払い口座に対応するユーザ情報によって初期化することである。好ましくは、これは、図5に示す前記支払いモジュールを使用するユーザによって行われる。ユーザは、前記キーパッド23を使用して情報を入力する。入力された前記情報は、前記支払いモジュールの例えばプログラム/情報格納装置28に格納される。指示、メニューおよびプロンプトは、(例えば、出力アダプタ29を介した)前記支払いモジュールとの通信によって、前記表示器40に与えられる。

【0037】図6の実施例において、前記支払いモジュールは、ステップ310において、第1のクレジットカードに対応する情報によって初期化される。典型的に

は、このクレジットカード初期化ステップ310で入力される情報は、トラック1またはトラック2のカードデータに対応する。前記トラック1またはトラック2のデータは、一般に、デビットカードまたはクレジットカードの磁気片にエンコードされている。磁気片リーダは、前記磁気片から情報を読み取ることが要求される。使用時において、カード所有者は、前記カードを前記磁気片リーダに通してカードデータを読み取らせる。典型的には、トラック1のデータは、カード所有者の名前、口座番号、有効期限終了日およびカード有効性確認値(CVV)または個人認識番号有効性確認値(PVV)に対応する。前記カード有効性確認値(CVV)および個人認識番号有効性確認値(PVV)は、周知の技術を使用して他の情報を検査確認するために使用されるものであり、一般に、前記磁気片上のその他のデータに対応するデータ値であって、カード発行者によって発生される。トラック2のデータは、典型的には、トラック1のデータと同じであるが、カード所有者の名前を含まない。

【0038】ステップ310で入力されたユーザ情報は、トラック1のデータもしくはトラック2のデータまたはこれらの両方、または、その他の情報セットに対応してよい。この情報は、ユーザによって前記支払いモジュールに入力される。好ましくは、カード発行者は、ユーザ10に対して、該ユーザが前記支払いモジュールに入力する数字列を提供する。この数字列は、前記ステップ310で入力すべきユーザ情報に対応する。好ましい実施例において、前記支払いモジュールは、前記表示器40に対して、図式メニューおよびプロンプトに対応する信号を送り、これにより、ステップごとの処理においてユーザがデータ入力する操作を案内する。こうして、データが入力されると、検査確認処理(ステップ320)が行われる。典型的な検査確認処理は、前記ユーザ情報が正確に入力されたか否かを調べるためにユーザによって文字が入力される論理的冗長検査を使用する。エラーが検出された場合、前記支払いモジュールによってデータ訂正シーケンス(ステップ330)が要求される。エラーが検出されなかった場合、この初期化処理は次のステップに行く。

【0039】次のステップ340において、ユーザは、初期化中のカードに関する暗号化された個人識別番号(PIN)を入力するよう指示される。該暗号化された個人識別番号は、任意の処理ステップ345によって提供されてよい。好ましい実施例において、ユーザには、上述のようなペーパー暗号化手段が提供される。該ペーパー暗号化手段は、好ましくはカード発行者によって維持される暗号化キーを使用して暗号化された個人識別番号を発生するために使用される。前記暗号化キーは、前記支払いモジュール上に維持されないのが好ましい。これにより、前記支払いモジュールに対する悪意のアクセスによつては、前記暗号化キーは発生されない。前記暗号化さ

れた個人識別番号は、表示器 40 に与えられる指示に従ってユーザによって前記支払いモジュールに入力され、該モジュールに格納される。

【0040】次のステップ 350 において、その他の初期化すべきカードが在るか否かを調べる。その他の初期化すべきカードが在る場合、処理ライン 360 によってステップ 310 に戻り、前記他のカードを上記ステップ 310～350 の処理によって、これを初期化する。その他の初期化すべきカードが無い場合には、最後の初期化ステップに行く。

【0041】この最後の初期化ステップ 370 において、ユーザは、前記支払いモジュールに対するアクセスを制御するために使用される支払いモジュールパスワードを選択するよう指示される。このようにして、支払いモジュールパスワードは、前記支払いモジュールに入力され、例えば前記プログラム/情報格納装置 28 に格納される。前記支払いモジュール 20 は、前記支払いモジュールパスワードの入力を必要とすることなく、前記表示器 40 またはインターフェイス/ケーブル箱 60 のためのリモートコントローラとして機能できるようになっているのが好ましい。同様に、前記支払いモジュールパスワードの入力によって、制限された支払い機能も可能になる。その代りに、前記支払いモジュールパスワードは、オーダシステムまたは支払いシステムに対するアクセスを可能にするためのものである。こうして、ユーザの支払い口座および暗号化された個人識別番号は、該ユーザのみによって使用可能になる。

【0042】代案として、前記支払いモジュールパスワードおよび支払い口座に関する情報は、2人以上のユーザによって入力されるようになっていてもよい。各ユーザの支払い口座に対するアクセスは、各々のユーザの支払いモジュールパスワードによって制限される。他の実施例において、前記支払いモジュールは、銀行のような処理センタにおいて、支払い口座情報によって初期化されてもよい。この実施例において、前記処理センタは、前記支払いモジュールにデータを送ることができるよう該モジュールに接続された磁気片リーダを備えている。こうして、該磁気片リーダは、前記初期化処理のための入力装置としてのキーパッド 23 の機能を補足または代替する。オペレータは、選択されたカードを前記磁気片リーダに通す。これは、前記磁気片リーダが、前記カードの磁気片からトラック 1 またはトラック 2 の情報のような所望の情報を読み取ることができるように行われる。こうして、前記磁気片リーダは自動的に前記所望の情報を前記支払いモジュールに出力し、該モジュールは上述の如く前記情報を格納する。さらに、ユーザは、例えば関連したキーパッドを使用することによって、所望の個人識別番号を入力してよい。こうして、前記磁気片リーダは入力された個人識別番号を処理して暗号化し、該暗号化された個人識別番号は、前記支払いモジュール

に送られて格納される。

【0043】この支払いモジュールを使用して、様々な金融取引を行うことができる。図 7 に示す典型的な取引において、ユーザは商品またはサービスを購入することができる。また、前記支払いモジュールは、例えば請求書に対する支払いを行ったり、様々な口座の間における資金移動を行ったりするための、電子的資金移動に使用されることもできる。

【0044】これらの取引に共通なのは、前記支払いモジュールの金融取引機能にアクセスするために入力可能な支払いモジュールパスワードを除いて、ユーザによる情報すなわち非暗号化された個人識別番号の入力を必要とすることなく、(トラック 1 またはトラック 2 のデータのような) 口座情報および暗号化された個人識別番号が、前記支払いモジュールによって自動的に提供されることである。これにより、ユーザが記憶して取り扱わなければならない支払いモジュールパスワードおよび個人識別番号の数を、減少することができる。

【0045】使用時において、購入取引は、前記表示器 40 に現れる対話型のプロンプトのシーケンスによって案内される。これらのプロンプトは、前記支払いモジュール 20 によって提供されるのが好ましいが、前記ネットワークを介して遠隔位置から提供されてもよい。典型的な取引において、ユーザは、ステップ 400 に示されるように、自分の支払いモジュールパスワードを入力するよう案内される。そして、ユーザは、プロンプトおよびメニューを参照しながら、特定の取引を選択する。

【0046】購入のためには、所望の品目が特定される。例えば、ユーザは、ステップ 410 において(例えば、商品コードを入力することによって)商品またはサービスを特定し、ステップ 420 においてその数量を特定する。そして、好ましくは、ユーザは、ステップ 430 において、所望の購入品目に対応する金額を確認するよう案内される。ユーザが前記金額に納得しない場合、所望の品目を再選択できるようステップ 410 に戻る。

【0047】前記金額が確認された後、ユーザは、ステップ 440 において、支払い方法を選択する。この支払い方法は、前記支払いモジュールを初期化した時に使用した支払い口座のうちの 1 つである。例えば、ユーザは、前記支払いモジュールを初期化した時に使用したクレジットカードまたはデビットカードのうちのいずれかを選択することができる。好ましくは、ユーザは、前記表示器 40 に表示されたメニューを見ながら、キーパッド 23 上の適当なキー押すことによって所望の支払い口座を選択する。

【0048】次に、一層の安全化のために、前記支払いモジュールは、ステップ 450 において、前記選択された支払い方法に対応する予め暗号化された個人識別番号を再び暗号化する。このステップ 450 における暗号化

は、DUKPT技術を使用して行われるのが好ましいが、任意の暗号化技術を使用して行われてよい。同様に、ステップ450において、所望の口座情報が暗号化される。この口座情報は、トラック1もしくはトラック2のデータに対応していてもよいし、または、他の所望口座情報であってもよい。

【0049】このように二重に暗号化された個人識別番号および暗号化された口座情報は、ステップ460に示すように、前記対話型のネットワーク80を介して送信される。前記対話型のネットワーク80は、銀行の処理部のような処理機関90と通信可能に接続されているのが好ましい。ユーザ、または、在宅購入システムを提供しているエンティティが所望の処理機関を選択できるよう、複数の他の処理が前記ネットワーク80と接続されていてもよい。

【0050】ステップ500に示すように、前記暗号化された個人識別番号および口座情報は、前記ネットワーク80を介して、前記処理機関90によって受信される。こうして、ステップ510に示すように、該処理機関90は、前記口座情報から支払い口座を検査確認する。典型的には、該処理機関90は、データ処理システムによって前記暗号化された個人識別番号および口座情報を受信する。該データ処理システムは、前記暗号化された口座情報を解読する。そして、ステップ520において、該データ処理システムは、この解読された口座情報から、支払い口座番号を検出し、関連銀行または金融機関のような前記口座を維持している機関95を検出する。典型的には、支払い口座番号は各発行機関に特有の識別可能コードを含んでいるので、前記口座を維持している機関95は、口座番号から検出可能である。

【0051】そして、前記処理機関は、前記ネットワーク80を介して、前記暗号化された個人識別番号および（暗号化された、または、暗号化されていない）口座情報を前記支払い口座機関95に送信する。こうして、必要に応じて、前記支払い口座機関95は、ステップ530において、前記暗号化された個人識別番号および口座情報を解読する。典型的には、前記支払い口座機関95は、データ処理システムによってこれらのデータを受信する。該データ処理システムは、前記暗号化された口座情報を解読する。該口座番号および個人識別番号は検査確認されるのが好ましく、その後、前記支払い口座機関95は、ステップ540において、その取引きを受入れるかまたは拒絶するかを判定する。例えば、前記支払い口座機関95は、既存の口座番号のデータベースをチェ

ックすることによって、前記口座番号を検査確認してよく、また、前記個人識別番号を、その口座番号に割り当てられた個人識別番号に対応するか否かをチェックすることによって検査確認してよい。例えば購入取引きである取引きを受入れるか拒絶するかを判定に関して、前記支払い口座機関95は、その口座についてのクレジットの上限を考慮して前記所望の購入価格をチェックしてよい。前記購入価格がクレジットの上限を超えている場合、典型的には、その取引きは拒絶されることになる。

10 【0052】前記支払い口座機関95が取引きを受入れるかまたは拒絶するかを判定すると、受入れメッセージまたは拒絶メッセージが、前記ネットワーク80を介して前記ローカルシステムに返される。以上のようにして、遠隔金融取引きシステムが提供される。

【0053】

【発明の効果】以上のように、この発明は、高度に安全化された金融取引きを可能にするという優れた効果を奏する。

【図面の簡単な説明】

20 【図1】この発明に係る遠隔金融取引システムのローカルシステムの実施の形態を例示するイラスト図。

【図2】同遠隔金融取引システムの全体的システム構成例を示すブロック図。

【図3】同遠隔金融取引システムにおけるローカルシステムの一構成例を示すブロック図。

【図4】同遠隔金融取引システムにおけるローカルシステムの別の構成例を示すブロック図。

【図5】この発明に関連する支払いモジュールのシステム構成例を示すブロック図。

30 【図6】同支払いモジュールを初期化するための処理の一例を示すフローチャート。

【図7】この発明に従って購入取引を行うための処理の一例を示すフローチャート。

【図8】図7の購入取引処理に応じて遠隔のシステムで行われる処理手続の一例を示すフローチャート。

【符号の説明】

20 支払モジュール

22 リモコン装置

26 マイクロプロセッサ

40 28 プログラム／情報格納装置（メモリ）

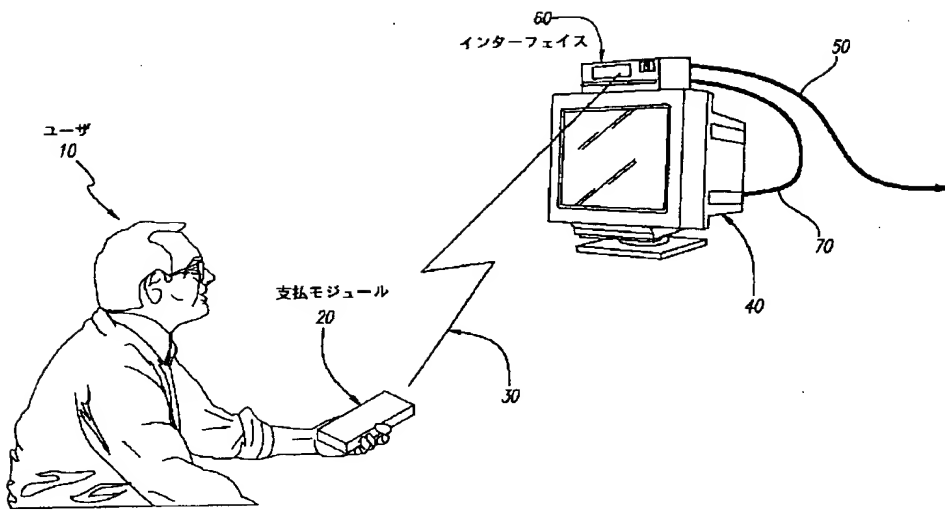
40 表示器

80 対話型のネットワーク

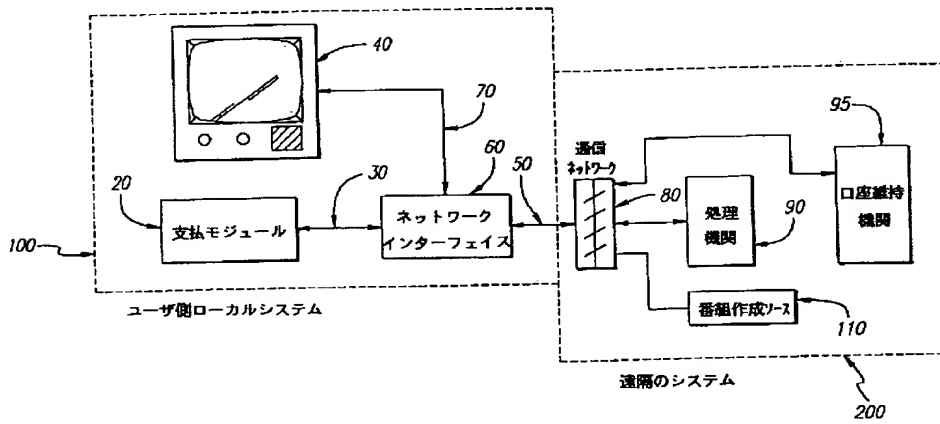
100 ローカルシステム

200 遠隔のシステム

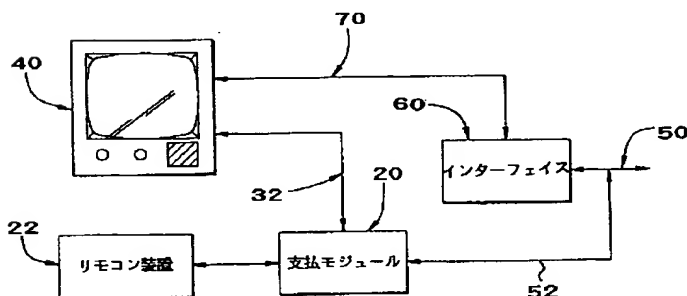
【図 1】



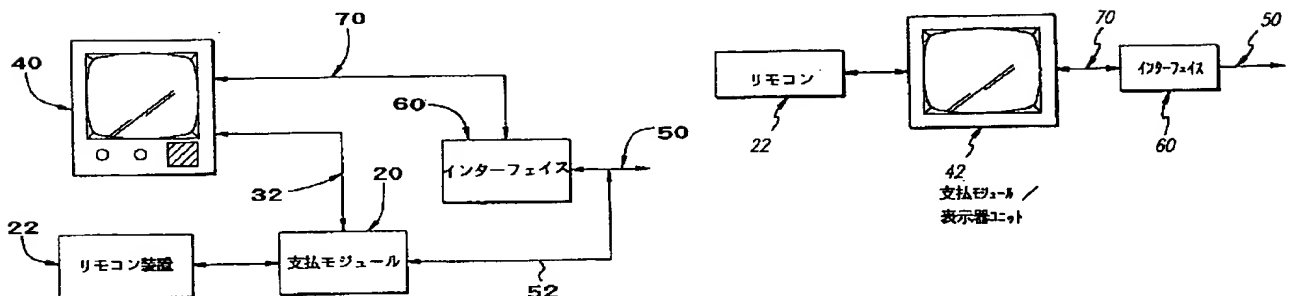
【図 2】



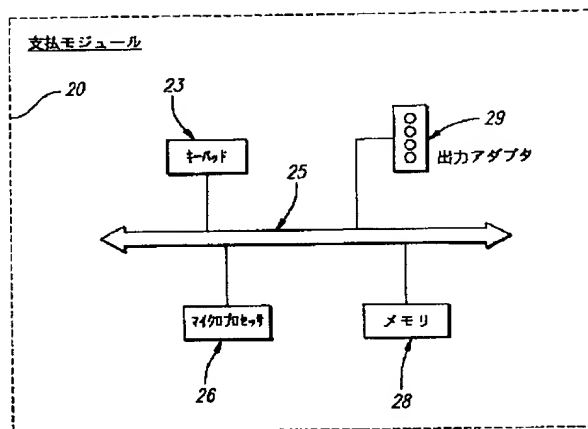
【図 3】



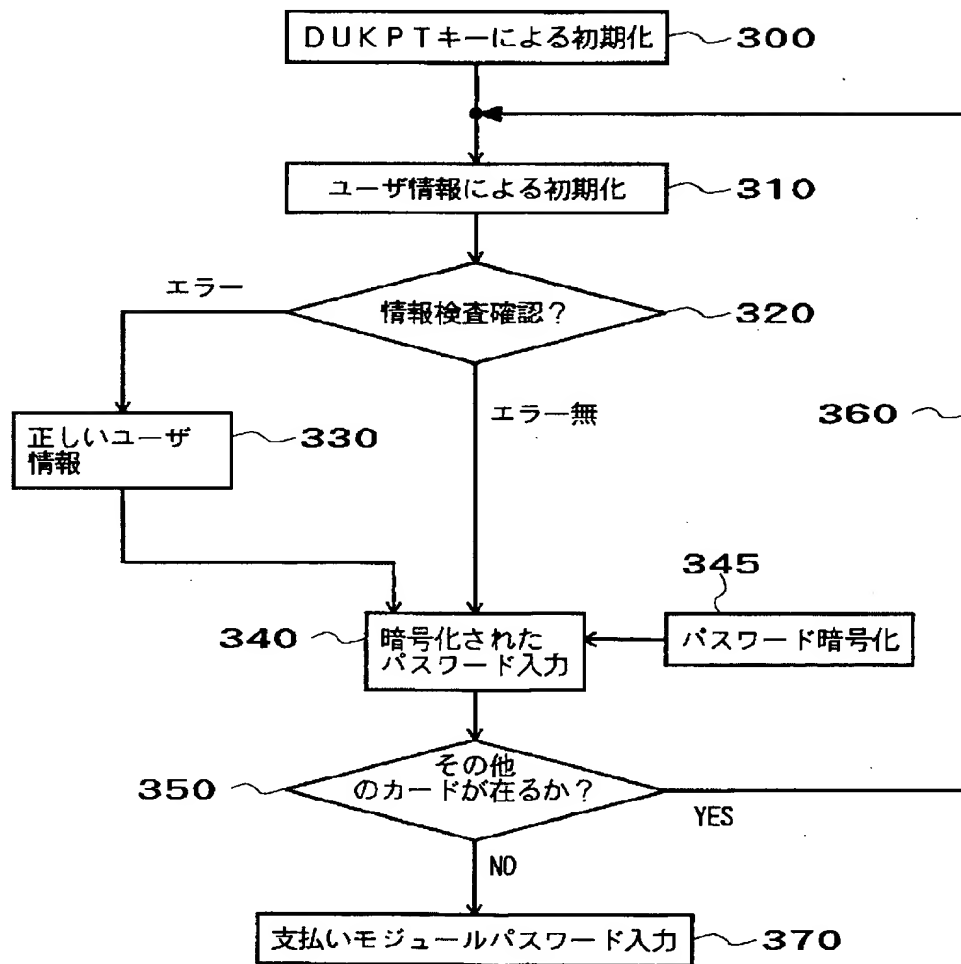
【図 4】



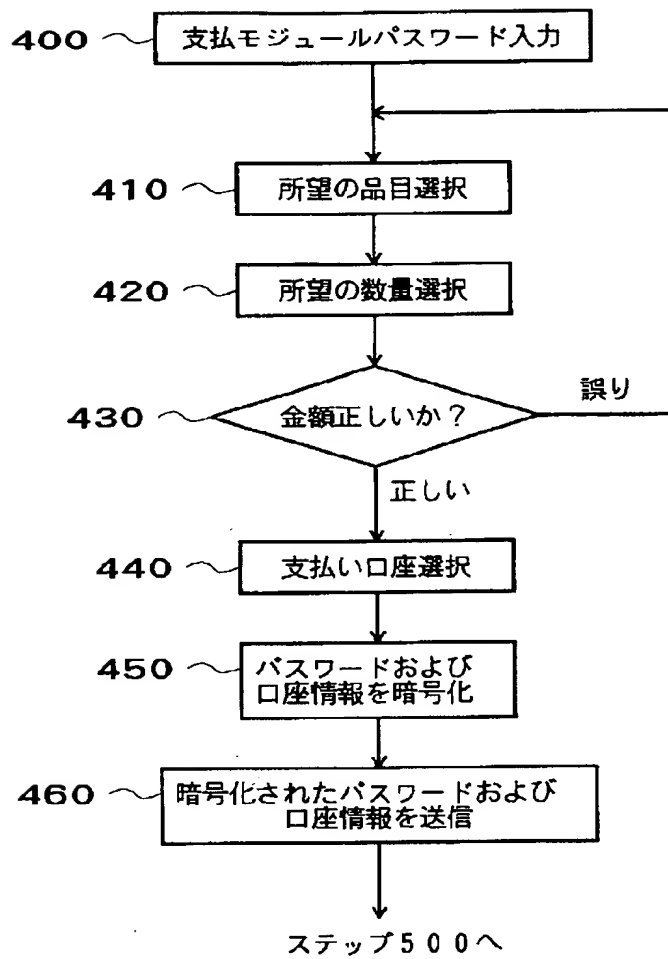
【図 5】



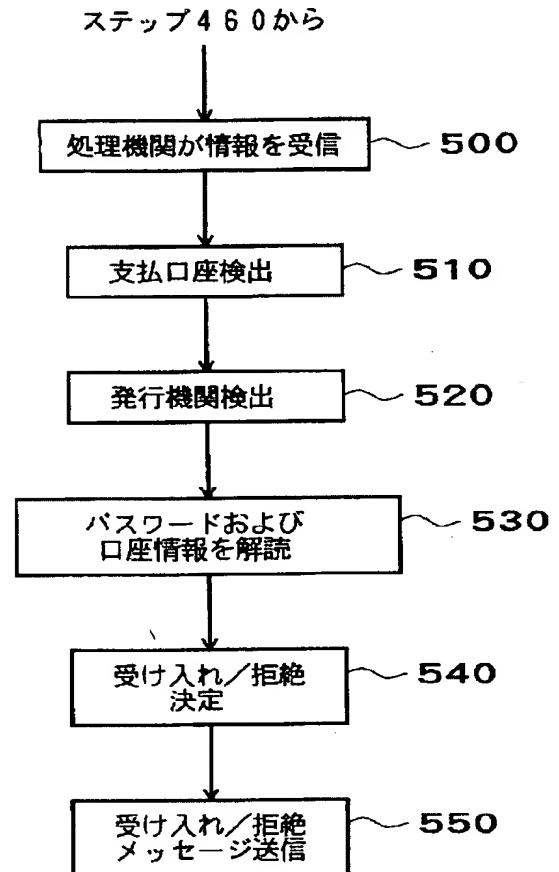
【図 6】



【図 7】



【図 8】



フロントページの続き

(51) Int. Cl. 6

識別記号

庁内整理番号

F I

技術表示箇所

G 0 7 D 9/00

3 6 0

4 7 6